Agència Nacional de Ciberseguretat d'Andorra

Conscienciació en ciberseguretat

Gestió de ciber-incidents de seguretat

Què és un incident o ciber-incident de seguretat?:

Parlem d'**incident de seguretat** o de **ciber-incident** quan un o diversos **successos** o **esdeveniments de seguretat** comprometen de manera **real** o **potencial** les operacions d'una organització, amenaçant d'atemptar la seva pròpia **seguretat**.
Un incident no té per què constituir necessàriament la materialització d'un **dany** o **perjudici**, sinó que pot considerar-se com a tal tota situació en la qual aquest mal pot arribar o no a materialitzar-se amb una **probabilitat** més o menys **significativa**.
considerem, doncs, que es tracten d'**incidents de seguretat** les accions següents:

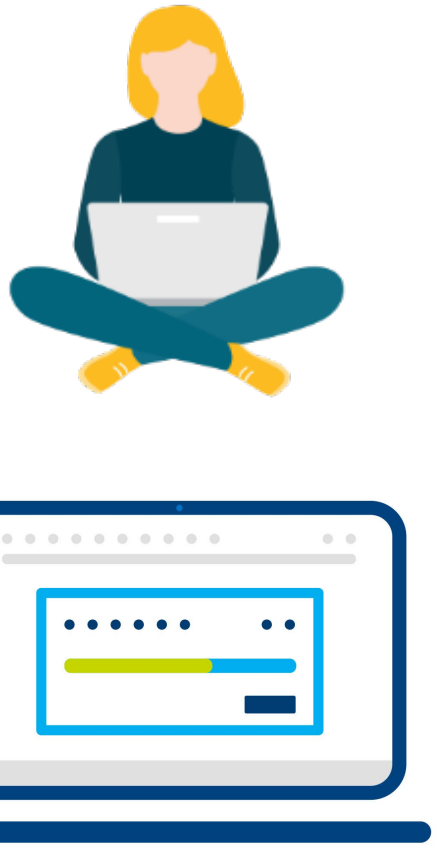
- Els successos o situacions que impedeixen el **correcte funcionament** de les **xarxes**, **sistemes** o **recursos tecnològics**.
- Els que posen en perill la **confidencialitat**, **integritat** o **disponibilitat** de qualsevol informació o d'un Sistema d'Informació.
- Els que constitueixin una **violació o amenaça** imminent de les **polítiques**, **normes** o **procediments de Seguretat de la Informació**.

Modalitats més habituals d'Incidents de Seguretat que ens podem trobar:

Alguns **exemples d'incidents de seguretat** que poden produir-se són:

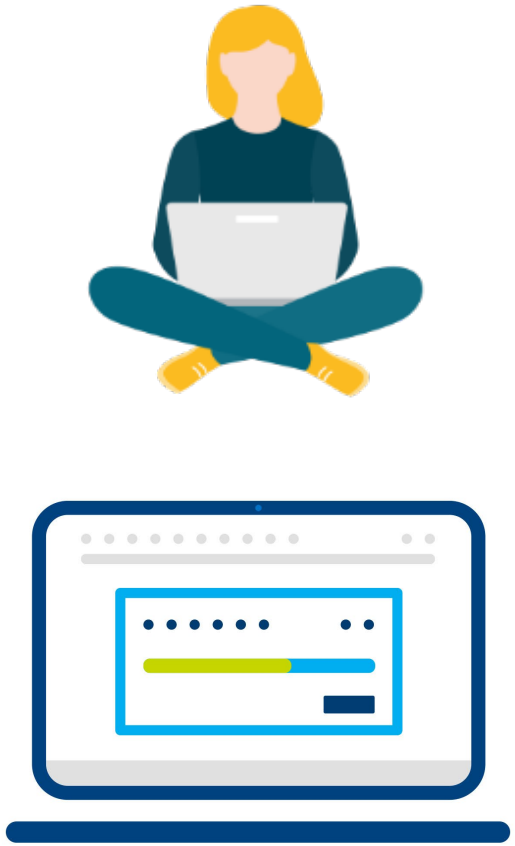
- **Accés no autoritzat** a informació confidencial.
- Pràctiques d'**enginyeria social** per aconseguir objectius il·legítims utilitzant l'engany.
- **Furt** d'informació confidencial, incloses les credencials dels usuaris.
- L'**alteració** o **supressió** d'informació confidencial per part del personal no autoritzat o per error.
- L'**abús** o **mal ús** dels sistemes d'informació de l'organització.
- La introducció de **codi maliciós** als sistemes (virus, troians, cucs…).
- La **denegació dels serveis** o **bloqueig dels sistemes** que causin la pèrdua d'informació.
- L'**afectació** dels **serveis** i **sistemes** fins al punt que s'arriba a vulnerar la seguretat i la confidencialitat establertes per l'organització.

Tipus de ciber-incidents de seguretat:



CLASSIFICACIÓ	TIPUS D'INCIDENT	DESCRIPCIÓ
Contingut abusiu	**Spam**	Correu electrònic no sol·licitat o inesperat i que normalment és distribuït massivament als usuaris amb interessos comercials o de difusió de certa informació (veraç o no).
Contingut abusiu	**Delictes d'odi / Distribució de continguts que afecten a les persones**	Distribució d'informació sobre persones que representa una afectació contra la seva integritat i privacitat i que, a més, comporta una il·legalitat per afectar els seus drets.
Contingut nociu	**Sistema infectat**	Sistema (equips o dispositius informàtics) que han estat infectats per malware, com pot ser un virus o un troià.
Obtenció d'informació	**Enginyeria social**	Atac basat en l'engany dirigit als usuaris amb objectius que poden variar des de l'obtenció d'informació confidencial a la consecució d'accions que requeririen d'una autorització específica.

Tipus de ciber-incidents de seguretat:



CLASSIFICACIÓ	TIPUS D'INCIDENT	DESCRIPCIÓ
Frau	**Phishing**	Els atacs de phishing s'identifiquen com una variant dels atacs d'enginyeria social, que es basen en l'engany a través de correu electrònic, normalment amb l'objectiu d'obtenir informació o una usurpació econòmica.
Frau	**Suplantació / Frau del CEO**	Activitat de suplantació d'una persona o empresa per a l'obtenció d'un benefici il·lícit. Normalment recolzant-se de vulnerabilitats tècniques de les eines i sense necessitat de disposar de comptes o mitjans legítims.
Compromís de la informació	**Pèrdua de dades**	Pèrdua d'informació per un esgarriament, robatori o destrucció accidental d'algun suport.
Compromís de la informació	**Accés o modificació no autoritzada de la informació**	Accés o modificació d'informació per un intrús que va fer ús d'un compte compromès o aprofitant alguna vulnerabilitat tècnica.

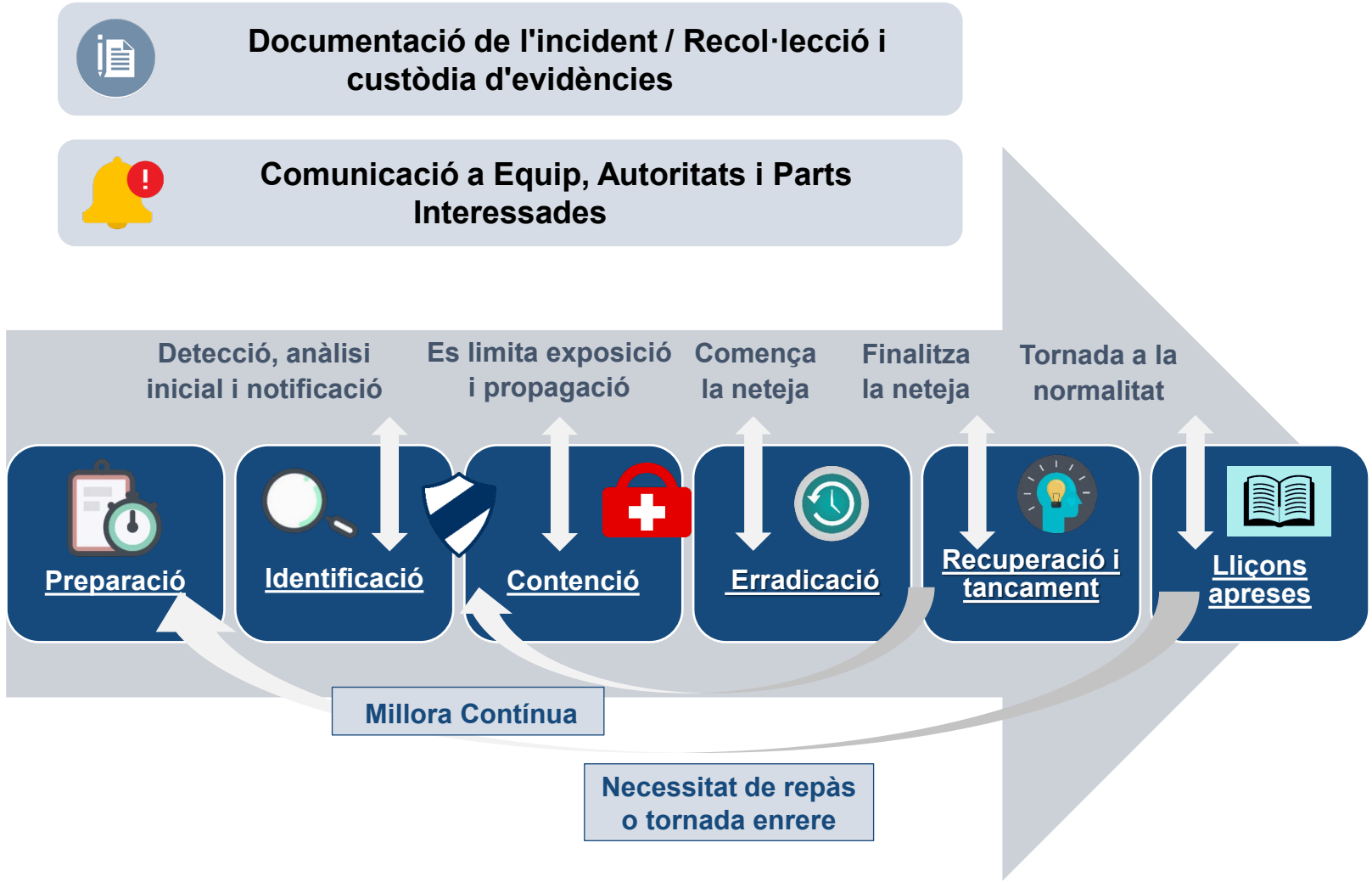
Tipus de ciber-incidents de seguretat:

CLASSIFICACIÓ	TIPUS D'INCIDENT	DESCRIPCIÓ
Compromís de la Informació / Vulnerabilitat	**Revelació**	Accés públic a sistemes o informació d'ús privat per una acció imprudent o una mala configuració.
Disponibilitat	**Sabotatge o interrupcions**	Atac dirigit a elements físics d'infraestructura com ara el cablejat, servidors. O també, desastres naturals que igualment deixen els sistemes fora de servei.
Intrusió	**Furt**	Sostracció de dispositius informàtics o informació que ocorre després de produir-se una intrusió física o una desprotecció.
Intrusió	**Intent d'accés amb vulneració de credencials**	Intents d'accés il·lícit a sistemes d'informació, perpetrant-hi normalment amb atacs de força bruta o amb una prova massiva de possibles credencials.

Protocol recomanable per la gestió dels ciber-incidents de seguretat:

En funció del **tipus** d'incident de seguretat que es produeixi, s'haurà d'iniciar un procediment per dur a terme la seva gestió. aquesta estarà composta per una sèrie de **fases** les quals es resumeixen en aquest **diagrama** i, per descomptat, tot això conforme els estàndards de referència ai bones pràctiques establertes en les diferents normatives que regulen aquesta matèria.

és important que els usuaris (els qui notifiquen així com altres afectats) entenguin que la gestió dels incidents de seguretat requereix en tot moment una **col·laboració activa** per part seva, tant per **proporcionar informació**, com per iniciar les **accions** que siguin necessàries, fins a la resolució d'aquest incident. d'aquí ve que, us recomanem sempre que els usuaris han de tenir coneixement sobre els procediments establerts a la seva organització en relació amb aquesta qüestió.



Principals tendències de ciber-incidents durant el 2022 a escala mundial:

Any rere any s'ha anat evidenciant un creixement considerable en relació amb el nombre d'incidents de ciberseguretat que es produeixen arreu del món. no obstant això, l'any 2022 ha estat un any especialment intens.

1. Guerra de Rússia contra Ucraïna

Actualment, les **ciberguerres** són atacs cibernètics que es cometen entre diversos països per mitjà de ciber-exèrcits. entre aquests atacs podem destacar atacs de tipus **ransomware**, campanyes de **phishing**, de **spamware**, de **denegació de servei** i de **malwares** destructius. aquests últims atacs (els de malware) tenien justament com a objectiu principal atacar a diferents entitats ucraïneses. de fet, el que van fer va ser **destruir** per complet tota la informació i propagar-se com una espècie de virus entre els diferents servidors i ordinadors dels ciutadans ucraïnesos.

2. Gestor de contrasenyes – LastPass

LastPass és un **gestor de contrasenyes** bastant popular en el món de la informàtica que va ser víctima l'any passat d'un important **ciberatac**. Els atacants van aconseguir accedir a les **còpies de seguretat** que guardaven en el seu entorn de Desenvolupament. No obstant això, la companyia va al·legar que les **dades** més **sensibles** com els usuaris i les contrasenyes es trobaven totalment **xifrats** i els atacants no havien pogut accedir a aquesta informació.

3. Atacs via Scams a entitats bancàries

El terme «**scam**» es refereix a tota mena d'**estafes** o **atacs fraudulents** que es fan mitjançant Internet. Aquest tipus d'atacs es cometen a través de webs que el que fan és **suplantar la identitat** del Sistema dels Bancs per tal d'obtenir les dades dels usuaris i les seves contrasenyes per després realitzar transferències bancàries en nom dels clients. Transferències que, en moltes ocasions, eren **impossible de cercar** i això redunda en esdevenir **irrecuperables**.